

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2005年4月14日 (14.04.2005)

PCT

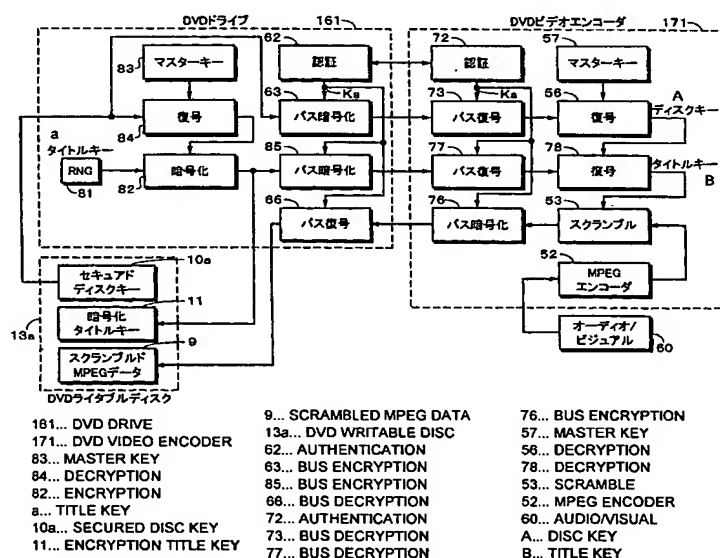
(10) 国際公開番号
WO 2005/034422 A1

- (51) 国際特許分類⁷: H04L 9/08, 12/14, G11B 20/10 (72) 発明者; および
(21) 国際出願番号: PCT/JP2004/013980 (75) 発明者/出願人 (米国についてのみ): 木谷 聡 (KITANI, Satoshi) [JP/JP]; 〒1410001 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社内 Tokyo (JP).
(22) 国際出願日: 2004 年 9 月 16 日 (16.09.2004) (74) 代理人: 杉浦 正知, 外(SUGIURA, Masatomo et al.); 〒1710022 東京都豊島区南池袋 2 丁目 49 番 7 号 池袋パークビル 7 階 Tokyo (JP).
(25) 国際出願の言語: 日本語 (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE,
(26) 国際公開の言語: 日本語
(30) 優先権データ: 特願2003-340076 2003 年 9 月 30 日 (30.09.2003) JP
(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒1410001 東京都品川区北品川 6 丁目 7 番 3 5 号 Tokyo (JP).

[続葉有]

(54) Title: SIGNAL PROCESSING SYSTEM

(54) 発明の名称: 信号処理システム



(57) Abstract: A writable disc (13a) where a secured disc key (10a) has been recorded in advance is used. A drive (161) includes inside itself: a random number generator (81) for generating a title key; an encrypter (82) for encrypting the generated title key with the disc key; a master key (83); and a decrypter (84) for decrypting the secured disc key with the master key. Furthermore, there are provided an authentication unit (62) for generating a session key (Ks), a bus encrypter (63) for encrypting the secured disc key with the session key (Ks), and a bus decrypter (66) for decrypting the scrambled MPEG data. Since the key for encryption is provided inside the drive, an ordinary user cannot create CSS write software as he/she desires.

(57) 要約: 予めセキュアドディスクキー 10a が記録されているライタブルディスク 13a が使用される。ドライブ 161 は、タイトルキーを生成する乱数発生器 81 と、生成したタイトルキーをディスクキーで暗号化するエンクリプタ 82 と、マスターキー 83 と、セキュアドディスクキーをマスターキーで復号するデクリプタ 84 とを内部に備えている。さらに、セッションキー Ks を生成する認証部 62、セッションキー Ks でセキュアドディスクキーを暗号化するバ

[続葉有]

WO 2005/034422 A1



SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US,
UZ, VC, VN, YU, ZA, ZM, ZW.

BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN,
TD, TG).

- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF,

添付公開書類:

— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。